Mesa 2

Nota : https://www.welivesecurity.com/la-es/2021/06/10/backdoordiplomacy-actualizando-quarian-turian-backdoor-utilizado-contra-organizaciones-diplomaticas/

¿Qué tipo de amenaza es? Malware Troyan backdoor

¿Cómo comienza y cómo se propaga esta amenaza?

Aprovecha la explotación de dispositivos vulnerables expuestos a Internet, como servidores web e interfaces de gestión para equipos de red. Una vez dentro de un sistema, sus operadores utilizan herramientas de código abierto para escanear el entorno y realizar movimiento lateral. Tiene como objetivo los medios extraíbles para la recopilación y exfiltración de datos.

¿Hay más de una amenaza aplicada ? Troyan, spyware

¿Qué solución o medida recomendarían ?

Crear copias de seguridad en dispositivos externos y reinstalar los sistemas operativos